IEEE MASS'24
Seoul, South Korea.

Khwarizmi Lab

Characterizing Encrypted Application Traffic Through Cellular Radio Interface Protocol

Md Ruman Islam[†], **Raja Hasnain Anwar**[*], Spyridon Mastorakis[‡], and Muhammad Taqi Raza[*]

[†]University of Nebraska Omaha, [*]University of Massachusetts Amherst, [‡]University of Notre Dame

September 23, 2024

University of Nebraska Omaha | University of Massachusetts Amherst | University of Notre Dame

Encrypted network traffic *ensures* no **eavesdropping**!

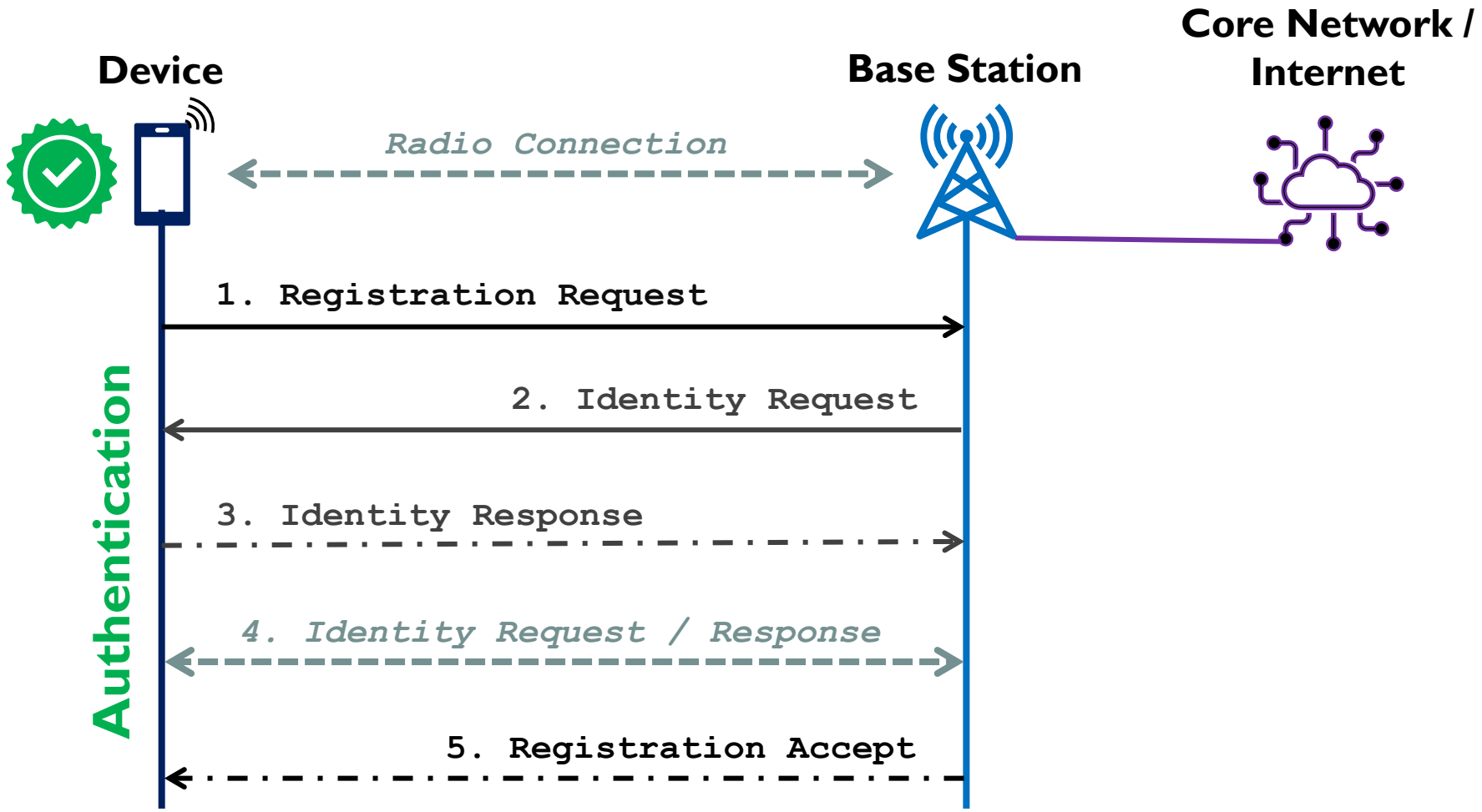
Encrypted network traffic
ensures no **eavesdropping**!

What if...

What if...

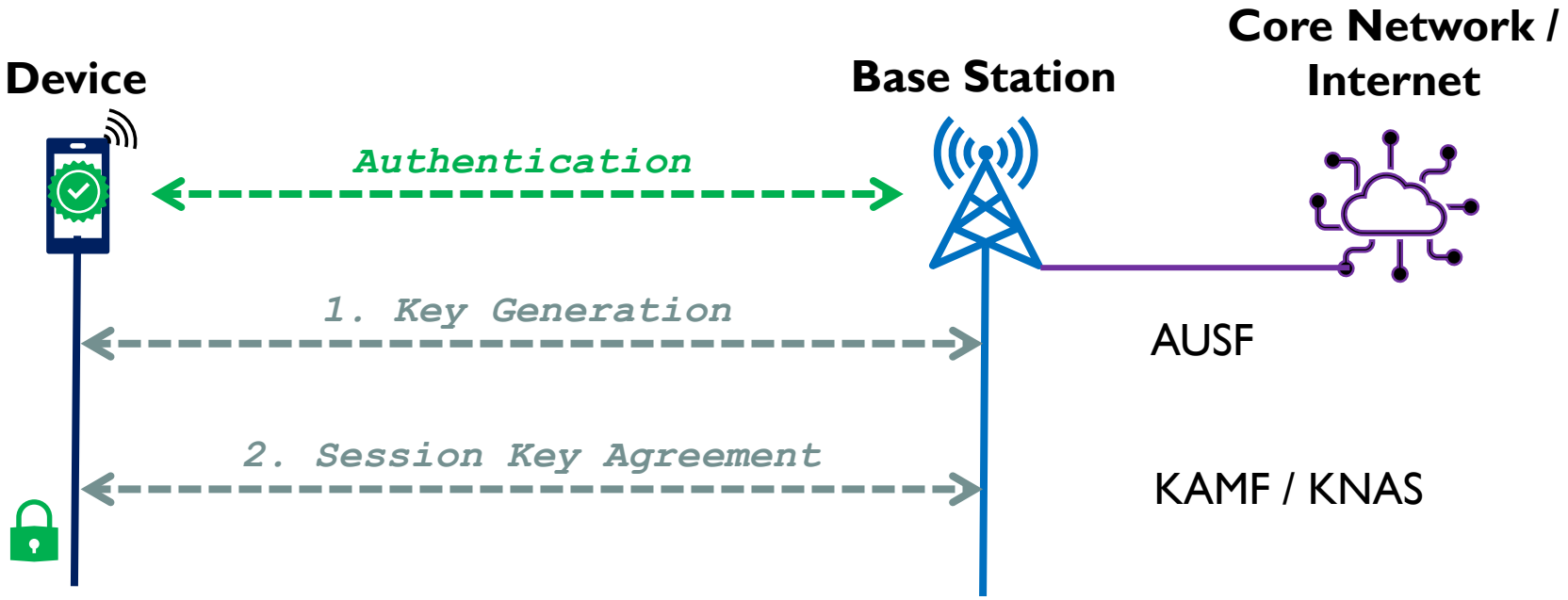
An adversary can still see what apps the user-device is using!!!

Understanding 5G: Device Registration



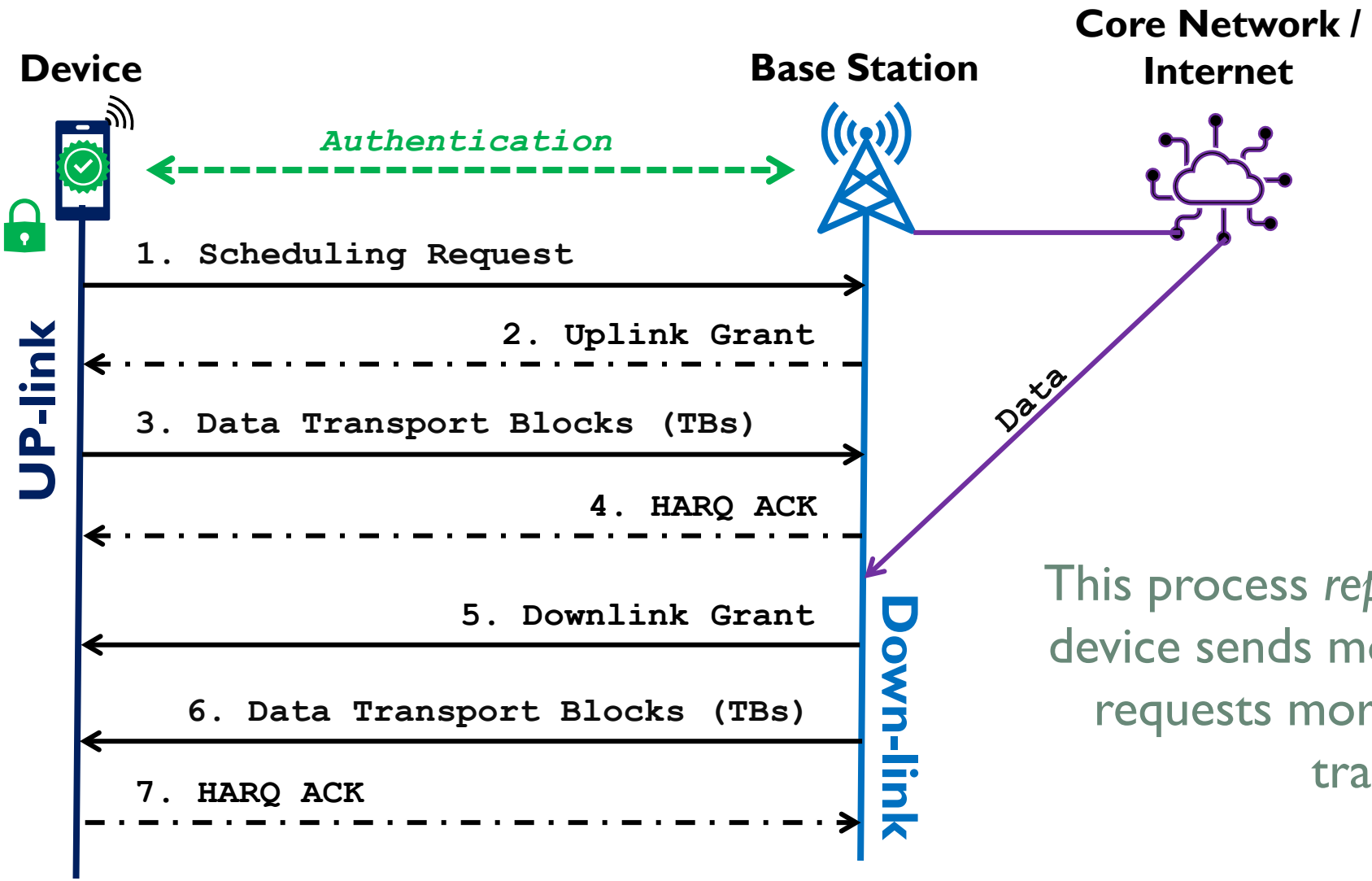
Every device needs to register and authenticate before accessing the 5G network.

Understanding 5G: Encryption Keys



The **NAS layer** encrypts all messages in subsequent exchanges, e.g., service requests, configuration updates.

Understanding 5G: Data Transmission



This process *repeats* as the device sends more data or requests more downlink transmissions.

Despite strong **authentication**, **encryption**, and **access control** mechanisms, how can an **adversary** learn about the **device's activities** over the network?

Research Question

Despite strong **authentication**, **encryption**, and **access control** mechanisms, how can an **adversary** learn about the **device's activities** over the network?

Radio Resource Blocks (RRBs) Allocation!

The Key Idea: Observing Physical and MAC layer Interactions

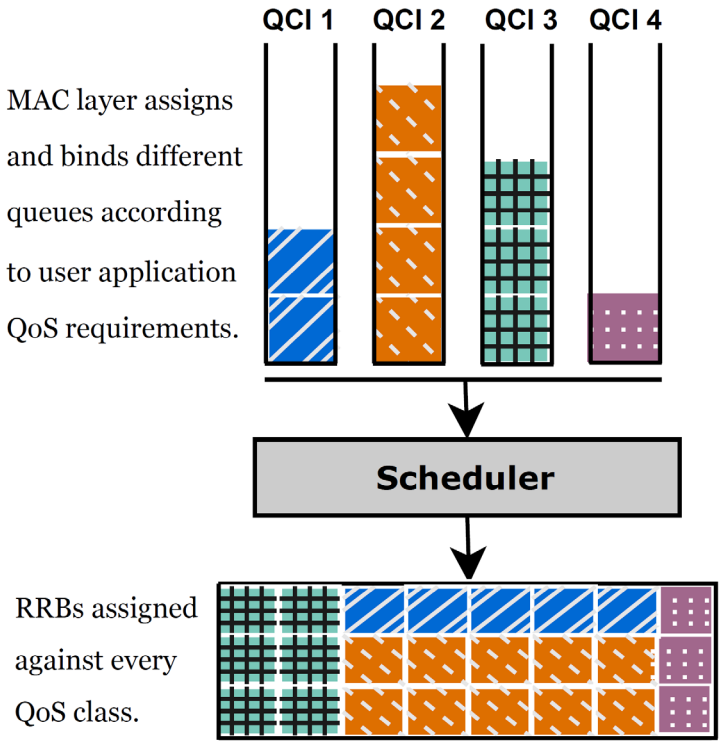
The device pushes data to the **PDCP layer**.

The **PDCP protocol** transfers the data to the **MAC layer**.

Stores the data in application-specific buffer for transmission.

The **MAC scheduler** requests the base station for radio resources:

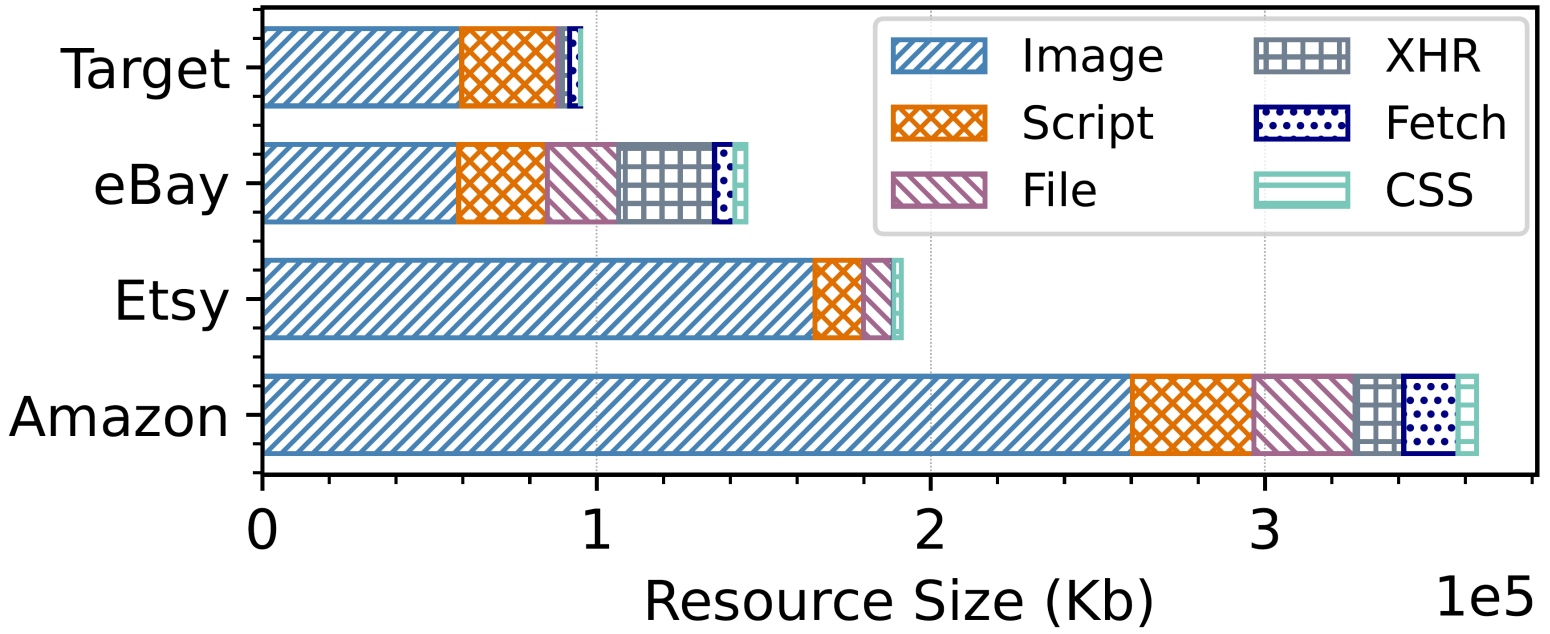
Buffer sizes	Quality-of-Service (QoS)	Priority



The device is running four different types of applications, e.g., voice call, web browsing, streaming, and real-time gaming.

MAC Scheduling

- There are 26 **QoS Class Identifiers (QCI)** indicating:
  - Guaranteed Bit Rate (GBR), or Non-GBR
  - Relative priority
- MAC layer assigns and binds different queues according to user application QoS requirements.
- The scheduler assigns RRBs against every QoS class.
  - It takes the *number*, *size*, and *priority* of different queues into account.



Key Insight: Unique Application Resources

How to acquire **scheduling** information for device-application **fingerprinting**?

Challenge 1

Acquiring Scheduling Information

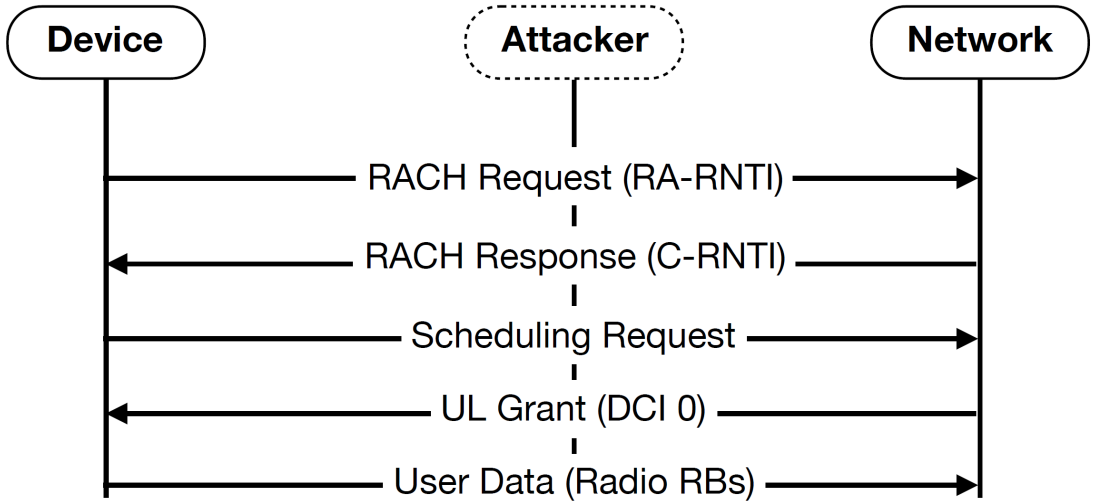
- **Downlink Control Information (DCI)** through the **Physical Downlink Control Channel (PDCCH).**
  - DCI Type 0: Uplink
  - DCI Type 1: Downlink
- Bitmap indicating the **Resource Block Groups (RBGs)** allocated to the device.
- The DCI is transmitted **without encryption** over the air.

- Eavesdrop on the **PDCCH** and retrieve the bitmap with **RBGs**.

How to identify the victim device?

Challenge 2

Identifying the Victim Device



- When a device registers with the network, it receives **C-RNTI**.
  - Unique device identifier within the cell.
  - Helps the device to identify the data intended for it.
- C-RNTI is sent in plaintext.
- The attacker can identify who is who over the radio communication.


5G
EXPERIMENTS,
EVALUATION, &
FINDINGS!

Experimental Setup

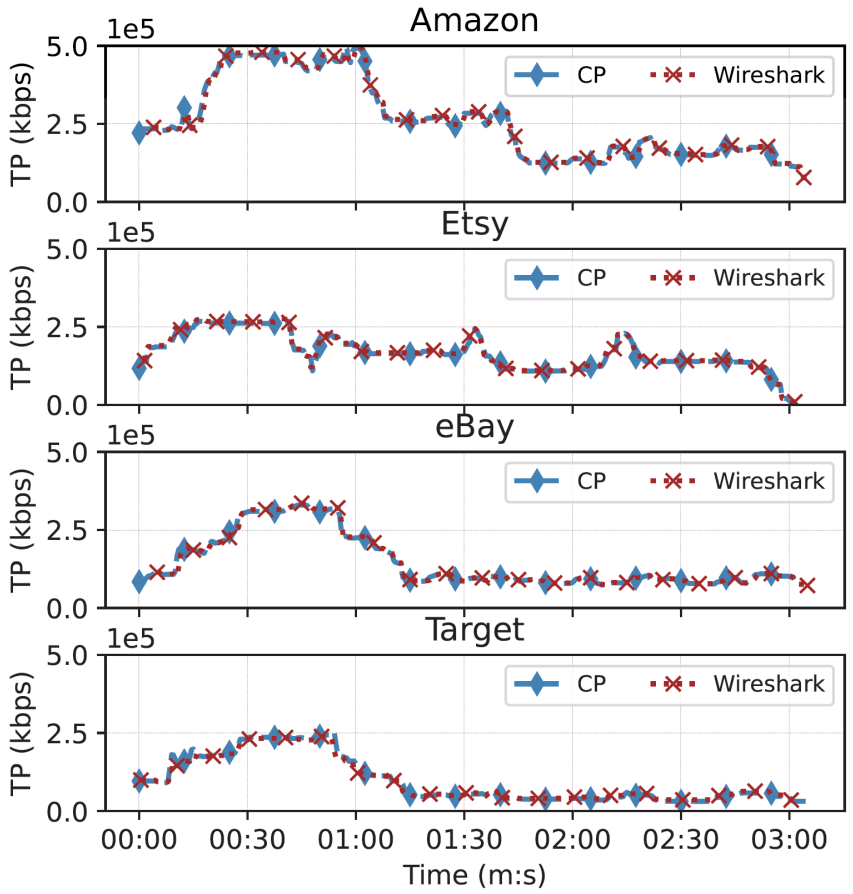
- OnePlus 5G cell phone.
  - Running multiple GBR and non-GBR applications.
  - Automated with Selendroid.
- **QXDM** and **QCAT** for collecting traces.
  - Radio Resource Block (RRB)
- We collect the traces for a single application at a time.
- 1217 traces over six-months.
  - >= 20 iterations per application.
  - 43 GBs!

Data Link

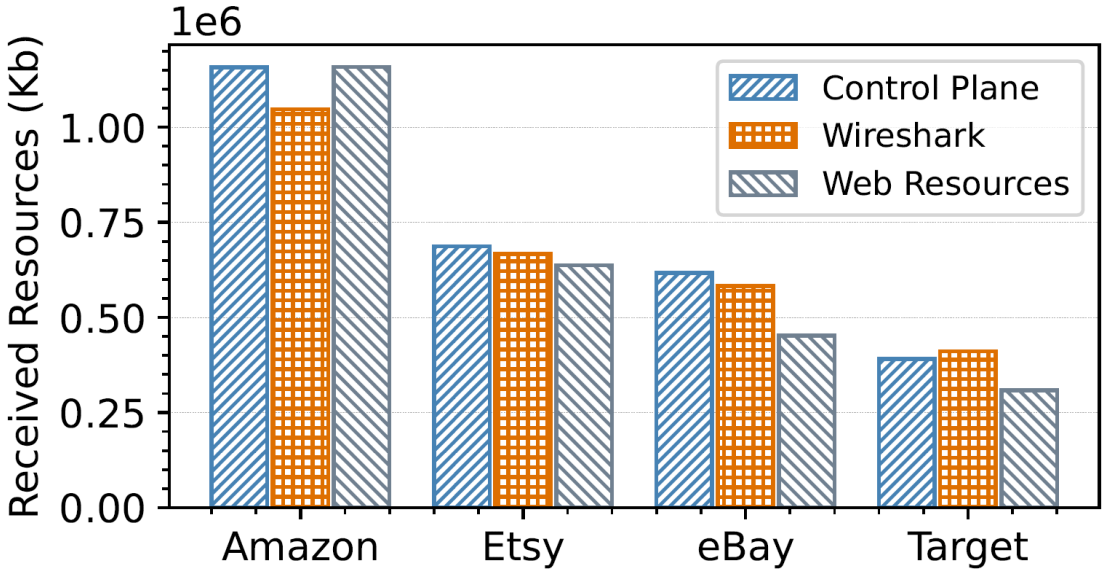
Service Category	Applications
Online Shopping	Amazon, eBay, Etsy, Target
Voice/Video Conferencing	Facebook Messenger, Telegram, WhatsApp, Zoom
Video Streaming	YouTube (Live and Non-Live in various qualities)
OTT Services	Apple TV+, Amazon Prime Video, Netflix

RRB vs. Device Wireshark

Continuous Usage

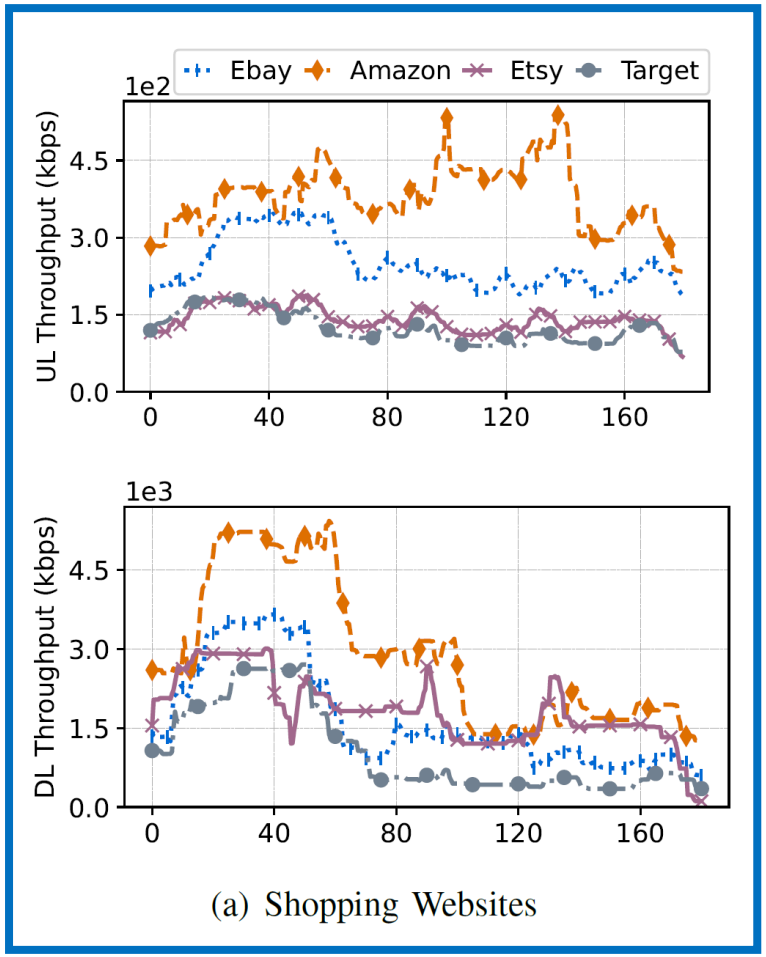


Total Usage

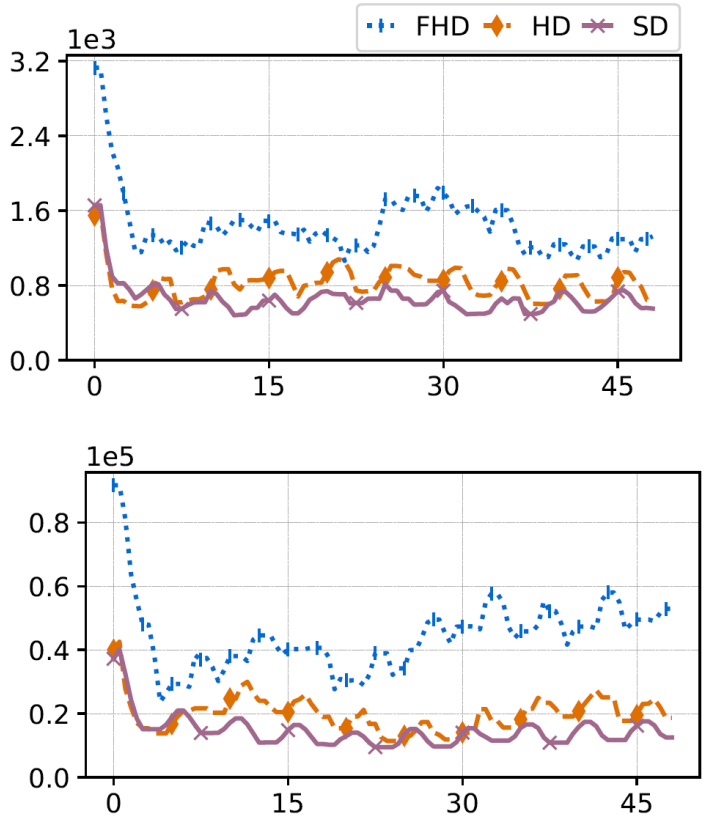


Throughput patterns in RRB and Wireshark are *identical* and *interchangeable*.

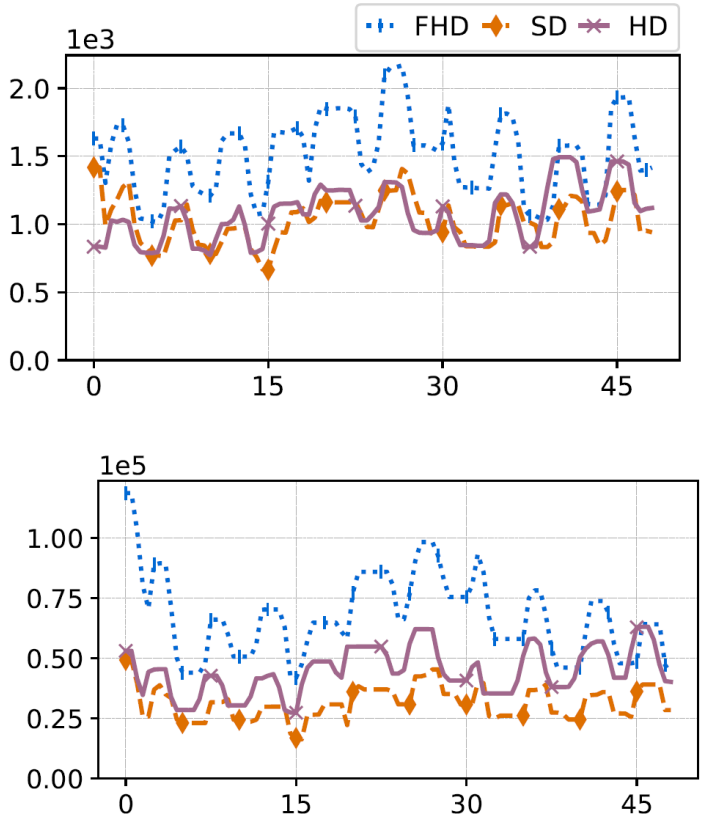
Fingerprinting Applications in the Wild



(a) Shopping Websites

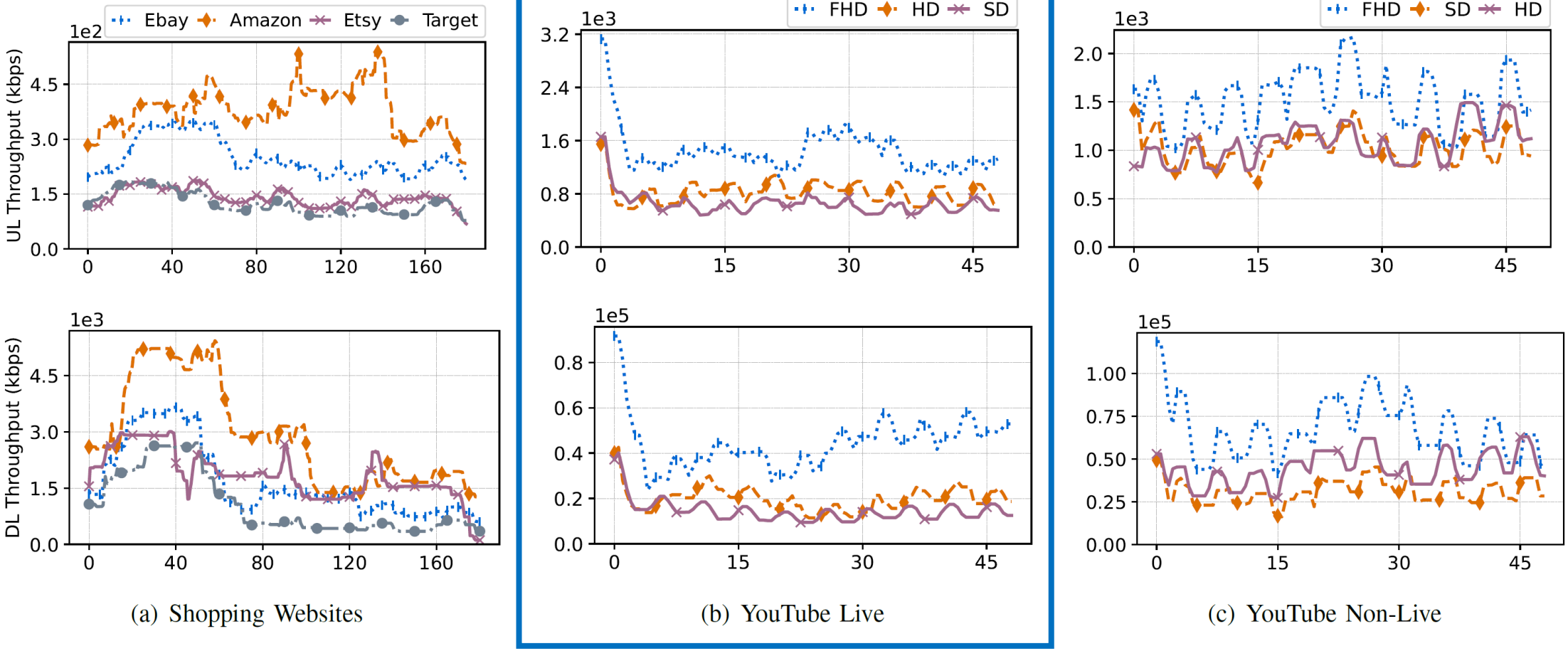


(b) YouTube Live



(c) YouTube Non-Live

Fingerprinting Applications in the Wild

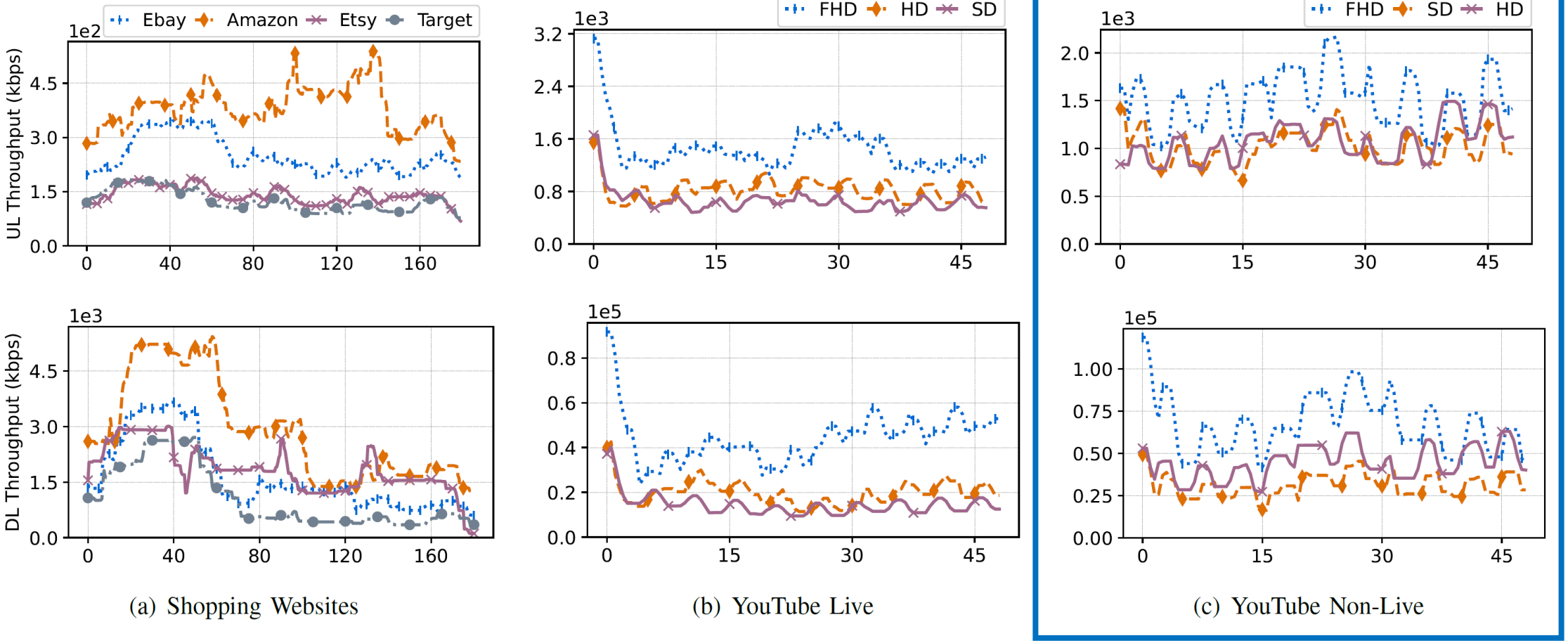


(a) Shopping Websites

(b) YouTube Live

(c) YouTube Non-Live

Fingerprinting Applications in the Wild

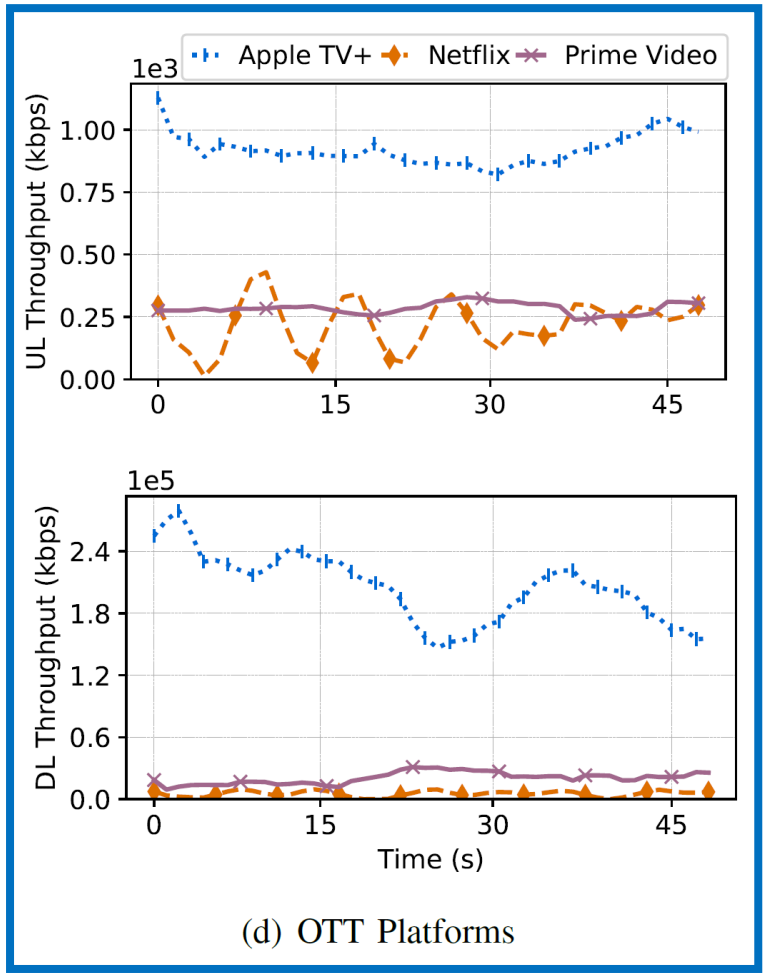


(a) Shopping Websites

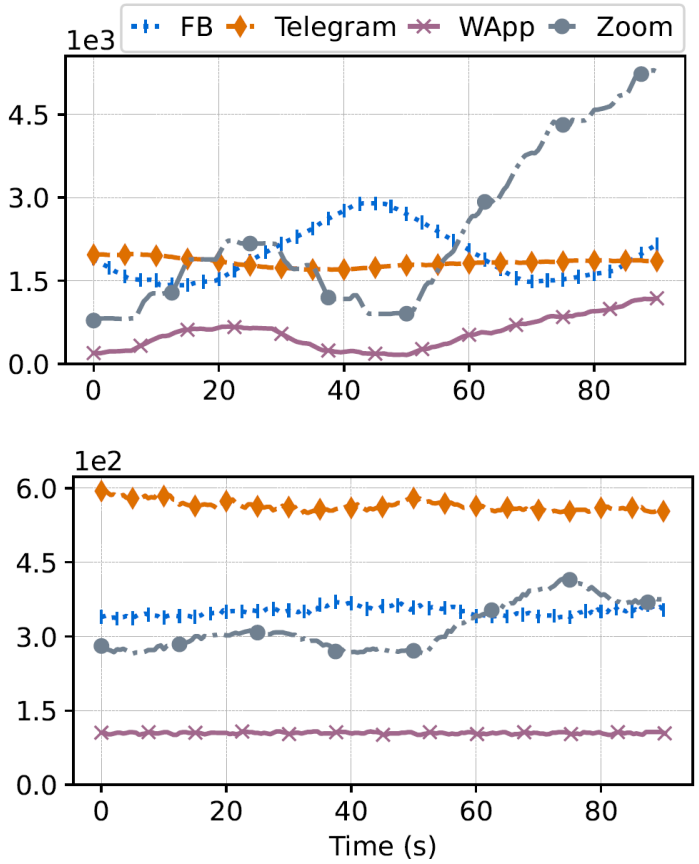
(b) YouTube Live

(c) YouTube Non-Live

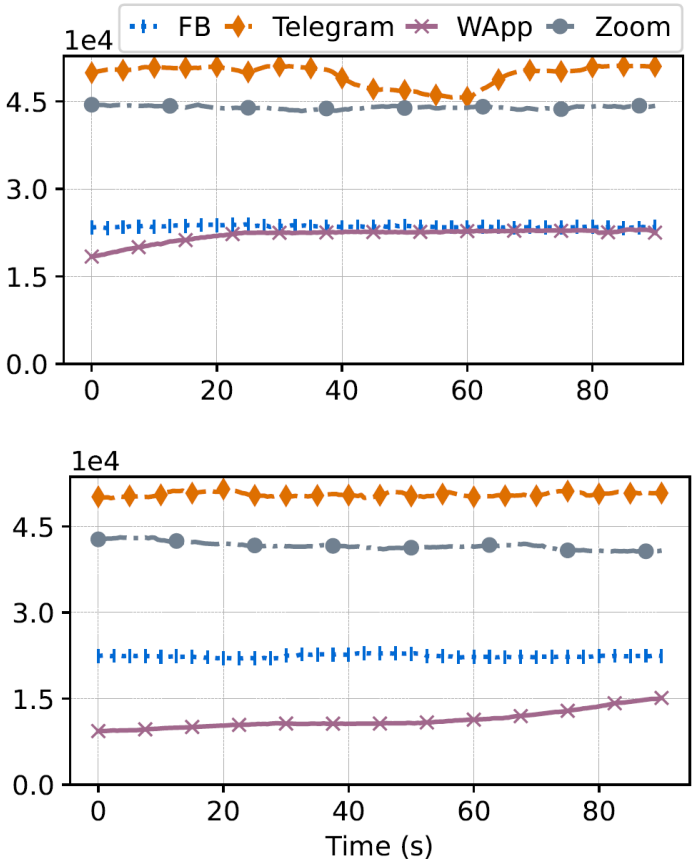
Fingerprinting Applications in the Wild



(d) OTT Platforms

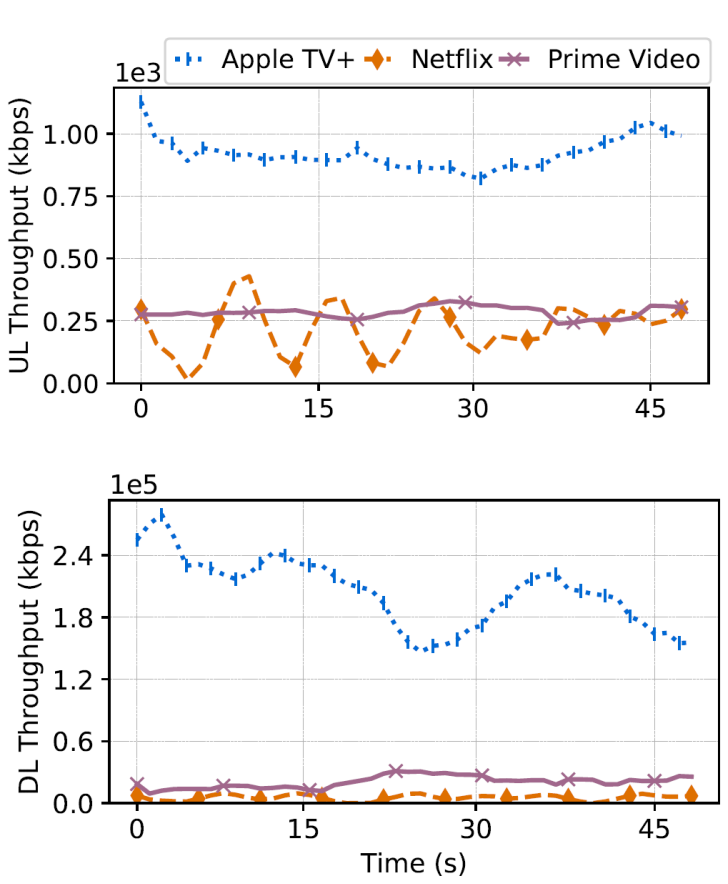


(e) Voice Call

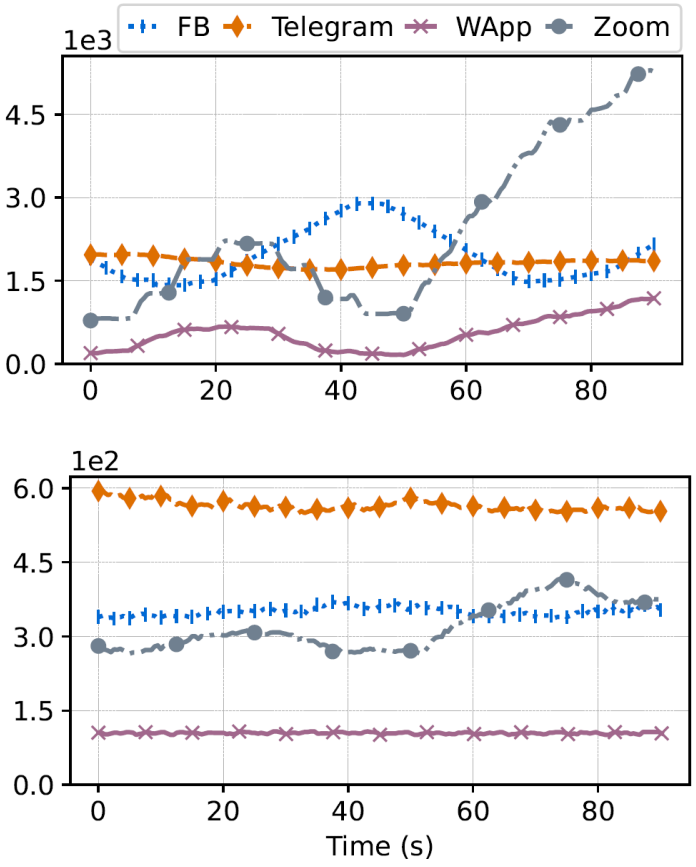


(f) Video Call

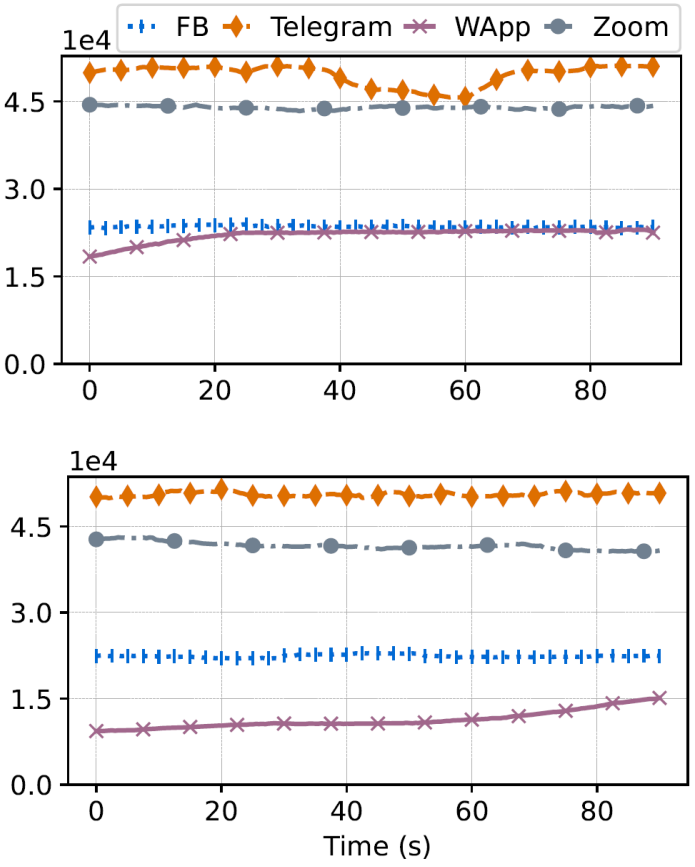
Fingerprinting Applications in the Wild



(d) OTT Platforms

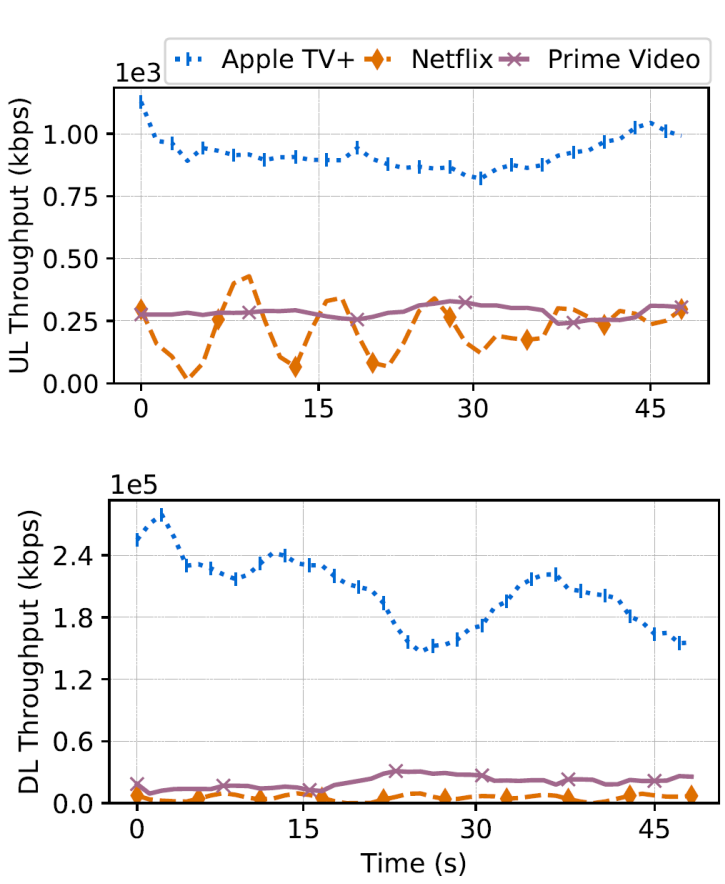


(e) Voice Call

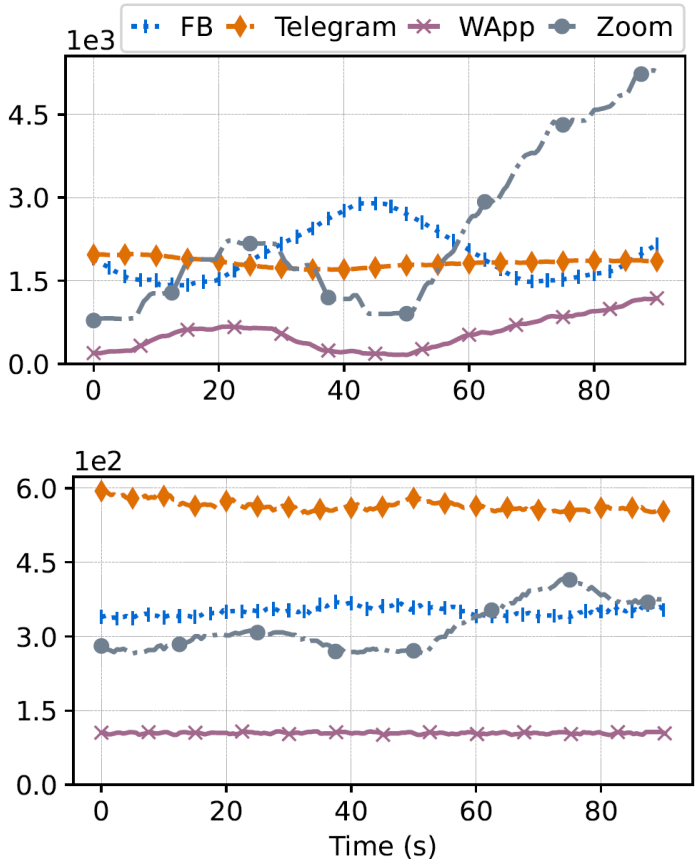


(f) Video Call

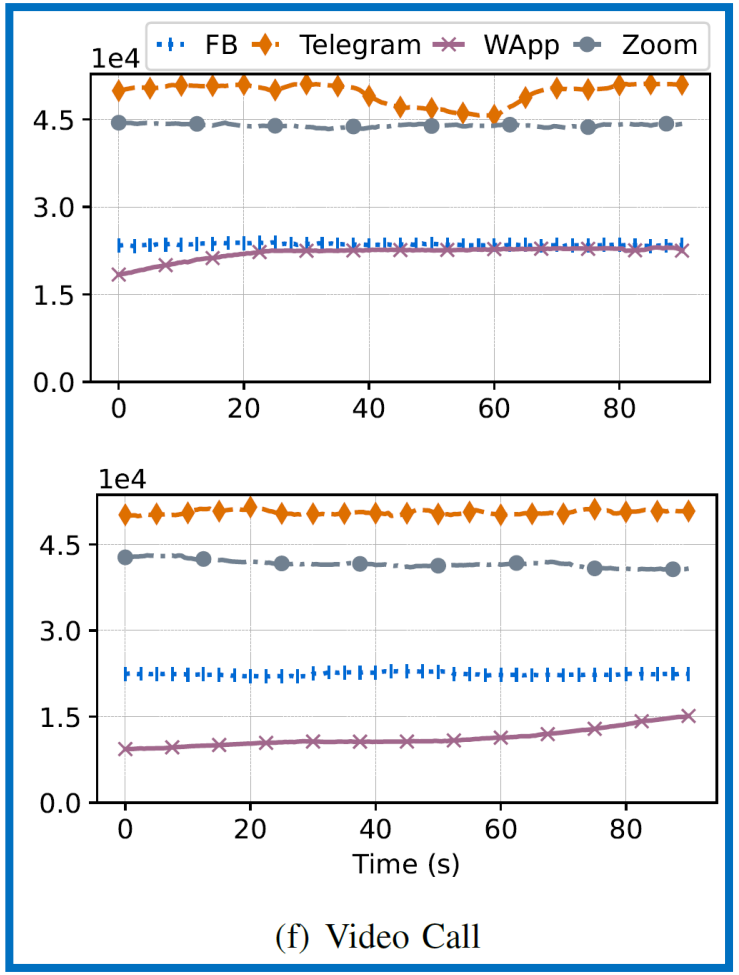
Fingerprinting Applications in the Wild



(d) OTT Platforms



(e) Voice Call



(f) Video Call

Application Classification

- **Random Forest** and **Extra Trees** classifiers for application and service category classification.
- We use similar hyperparameters and training setting for direct comparison.
- **Feature Generation:**
  - Min, Max, Mean, STD, Slope, Q1, and Q3

Models	Accuracy	Avg. Precision	Avg. Recall	Avg. F1-Score
Random Forest	94	93	94	93
Extra Trees	90	91	93	91

CONCLUSION

- We successfully fingerprinted various mobile applications in the wild using RRB traces.
- Our work highlighted the following insights:
  - Mobile applications generate **unique footprints** based on the number, types, and sizes of resources.
  - A correlation exists among the total resources, **RRB, and Wireshark** throughputs.
  - We can analyze both **continuous and cumulative** data to distinguish different types of applications.
- Our study aims to inform future design, implementation, and deployment decisions of 5G mobile networks and beyond.

Seeking internship opportunities!

Raja Hasnain Anwar

Email: ranwar@umass.edu

Web: rhasnainanwar.me

Khwarizmi Lab @ UMass

www.ecs.umass.edu/khwarizmi

Follow our research!

Lead Author

Md Ruman Islam

Email: mdrumanislam@unomaha.edu